Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research PROGNOSIS IP Telephony Manager 9.6 with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research PROGNOSIS IP Telephony Manager 9.6 to interoperate with Avaya Aura® Communication Manager 6.0.1.

PROGNOSIS IP Telephony Manager is a performance management solution for multi-vendor IP telephony solutions. PROGNOSIS IP Telephony Manager provides visibility of Avaya and other vendor's IP Telephony solutions from a single console. Targeted at multi-site enterprises and managed service providers of IP telephony solutions, PROGNOSIS IP Telephony Manager offers a multi-customer, multi-PBX perspective, enabling a significant reduction in complexity when managing complex IP telephony environments.

PROGNOSIS integrates directly to Communication Manager using Secure Shell (SSH). At the same time, it processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Integrated Research PROGNOSIS IP Telephony Manager with Avaya Aura® Communication Manager.

The PROGNOSIS IP Telephony Manager is based on the PROGNOSIS product-family architecture for the scalable monitoring of business critical systems. The PROGNOSIS product consists of:

- One or more PROGNOSIS Monitoring Nodes (Server Nodes). These are servers used by the PROGNOSIS product to collect, relay and store information collected from Communication Manager.

- The PROGNOSIS GUI is a Microsoft Windows client program which is used to connect to a PROGNOSIS Monitoring Node and display the information collected by the Monitoring Node. The PROGNOSIS GUI may either be installed on a Monitoring Node or on a separate computer.

The PROGNOSIS IP Telephony Manager product uses three methods to monitor a Communication Manager system.

- System Access Terminal (SAT) - The PROGNOSIS IP Telephony Manager uses a pool of SSH connections to the SAT using the IP address of the Avaya Server. By default, the solution establishes three concurrent SAT connections to the Communication Manager system and uses the connections to execute SAT commands.

- Real Time Transport Control Protocol (RTCP) Collection - The PROGNOSIS IP Telephony Manager collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones and IP Softphones.

- Call Detail Recording (CDR) Collection - The PROGNOSIS IP Telephony Manager collects CDR information sent by Communication Manager.

2. General Test Approach and Test Results

The general test approach was to use PROGNOSIS GUI to display the configurations of the Communication Manager systems and verify against what is displayed on the SAT interface. The SAT interface is accessed by using either telnet or Secure Shell (SSH) to the Avaya S8800 and S8300D Servers. Calls were placed between various Avaya endpoints and PROGNOSIS GUI was used to display the RTCP and CDR information collected.

2.1. Interoperability Compliance Testing

For feature testing, PROGNOSIS GUI was used to view the configurations of Communication Manager such as port networks, cabinets, media gateways, ESS, LSP, trunk groups, route patterns, CLAN, MEDPRO and DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. During testing, a call generator was used to load the Communication Manager systems by placing incoming calls through two E1 ISDN-PRI trunks to the system in Site A and terminating the calls as IP stations on the system in Site B. For the collection of RTCP and CDR information, the endpoints included Avaya IP, digital and analog telephones, Avaya A175 Desktop Video Device and Avaya one-X® Communicator users. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, transferred calls and conference calls.

For serviceability testing, reboots were applied to the PROGNOSIS IP Telephony Manager Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8800 Servers and failover to ESS and LSP were also performed during testing.

2.2. Test Results

All test cases passed successfully.

2.3. Support

For technical support on Integrated Research PROGNOSIS IP Telephony Manager, contact the Integrated Research Support Team at:

- Hotline: +61 (2) 9921 1524
- Email: support@prognosis.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Integrated Research PROGNOSIS IP Telephony Manager interoperability with Communication Manager. It consists of a Communication Manager system running on a pair of Avaya S8800 Servers with two Avaya G650 Media Gateways, an Avaya G430 Media Gateway with Avaya S8300D Server as a Local Survivability Processor (LSP) and an Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) running on Avaya S8800 Server was also configured for failover testing. A second Communication Manager system runs on an Avaya S8300D Server with an Avaya G450 Media Gateway. Both systems have Avaya IP (H.323 and SIP), digital and analog telephones, and Avaya one-X® Communicator users configured for making and receiving calls. IP Trunks connect the two systems together to allow calls between them. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP telephones and Avaya A175 Desktop Video Device. Integrated Research PROGNOSIS IP Telephony Manager was installed on a server running Microsoft Windows Server 2003 with Service Pack 2. Both the Monitoring Node and GUI software are installed on this server. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, media gateways and IP telephones.

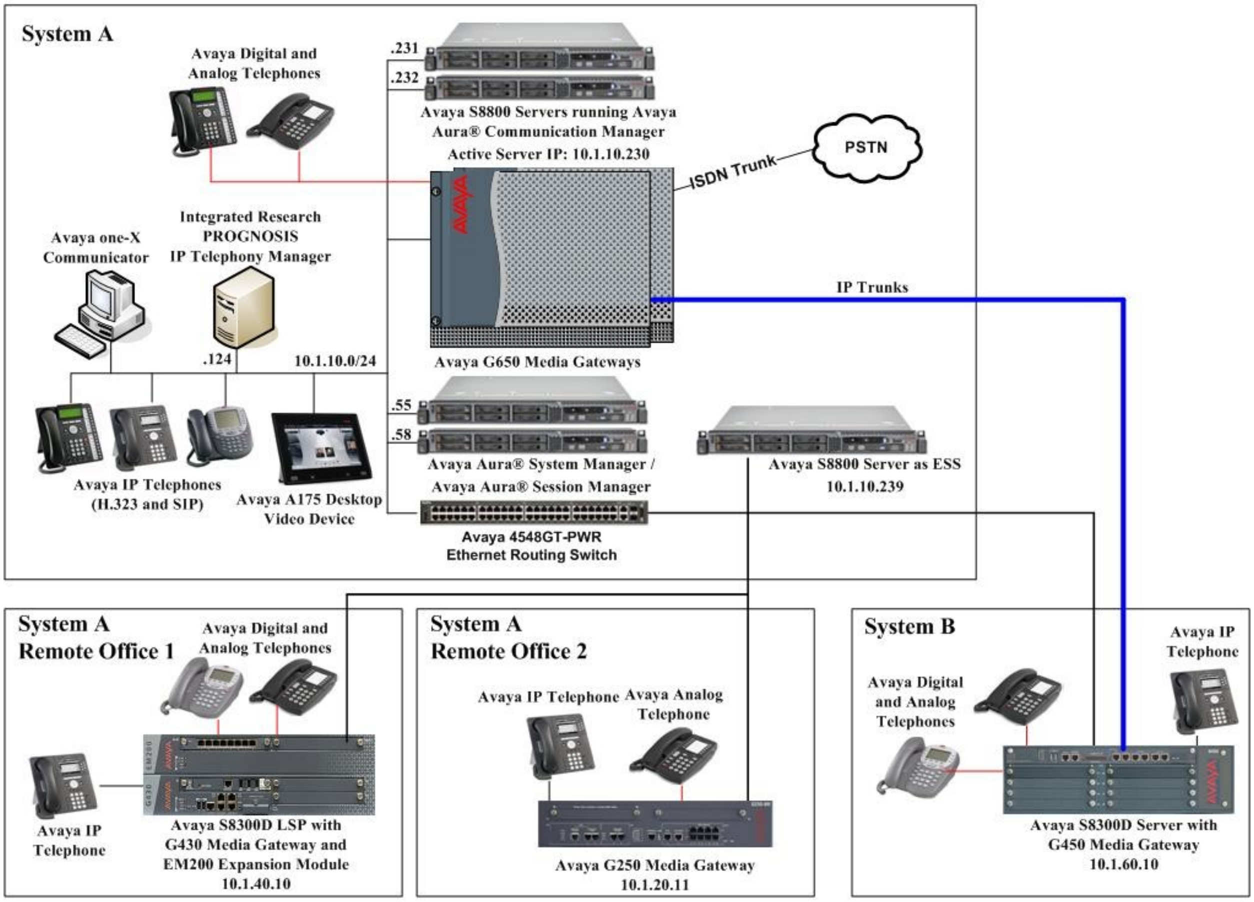

System A
Avaya Digital and Analog Telephones
.231
.232
Avaya S8800 Servers running Avaya Aura® Communication Manager
Active Server IP: 10.1.10.230
ISDN Trunk
PSTN
Integrated Research PROGNOSIS IP Telephony Manager
Avaya one-X Communicator
IP Trunks
.124
10.1.10.0/24
Avaya G650 Media Gateways
.55
.58
Avaya IP Telephones (H.323 and SIP)
Avaya A175 Desktop Video Device
Avaya Aura® System Manager / Avaya Aura® Session Manager
Avaya S8800 Server as ESS
10.1.10.239
Avaya 4548GT-PWR Ethernet Routing Switch
System A Remote Office 1
Avaya Digital and Analog Telephones
Avaya IP Telephone
Avaya S8300D LSP with G430 Media Gateway and EM200 Expansion Module
10.1.40.10
System A Remote Office 2
Avaya IP Telephone
Avaya Analog Telephone
Avaya G250 Media Gateway
10.1.20.11
System B
Avaya Digital and Analog Telephones
Avaya IP Telephone
Avaya S8300D Server with G450 Media Gateway
10.1.60.10

Figure 1: Test Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8800 Servers	Avaya Aura® Communication Manager 6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya G650 Media Gateways	-
- TN2312BP IP Server Interface	HW07, FW053 and HW15 FW054
- TN799DP C-LAN Interface	HW01, FW039 and HW01 FW040
- TN2302AP IP Media Processor	HW20 FW121 and HW20 FW117
- TN2602AP IP Media Processor	HW02 FW058 and HW02 FW041
- TN2214CP Digital Line	HW08 FW015
- TN793CP Analog Line	HW09 FW010
- TN2464BP DS1 Interface	HW05 FW024
- TN2464CP DS1 Interface	HW02 FW024
Avaya G250-BRI Media Gateway	30.18.1
Avaya G430 Media Gateway	31.18.1
- MM712AP DCP MM	HW04 FW009
- MM714AP Analog MM	HW04 FW073
- MM711AP Analog MM	HW31 FW093
- MM710AP DS1 MM	HW05 FW021
Avaya S8300D Server as LSP	6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya S8800 Server as ESS	6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya S8300D Server	Avaya Aura® Communication Manager 6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya G450 Media Gateway	31.18.1
- MM722AP BRI Media Module (MM)	HW01 FW008
- MM712AP DCP MM	HW07 FW009
- MM714AP Analog MM	HW10 FW093
- MM717AP DCP MM	HW03 FW009
- MM710BP DS1 MM	HW11 FW049
Avaya Aura® System Manager	6.1 Service Pack 2
Avaya Aura® Session Manager	6.1 Service Pack 2
Avaya 9600 Series IP telephones - 9630, 9640, 9650, 9670G	3.1 SP2 (H.323) or 2.6 SP4 (SIP)
Avaya 1608 IP telephones	1.300B (H.323)
Avaya 6221 analog telephones	-

Equipment	Software
Avaya digital telephones - 1416 - 2420	 SP1 -
Avaya A175 Desktop Video Device	1.0
Avaya one-X® Communicator	6.0 SP1 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
Integrated Research PROGNOSIS IP Telephony Manager	9.6.1 Patch 11

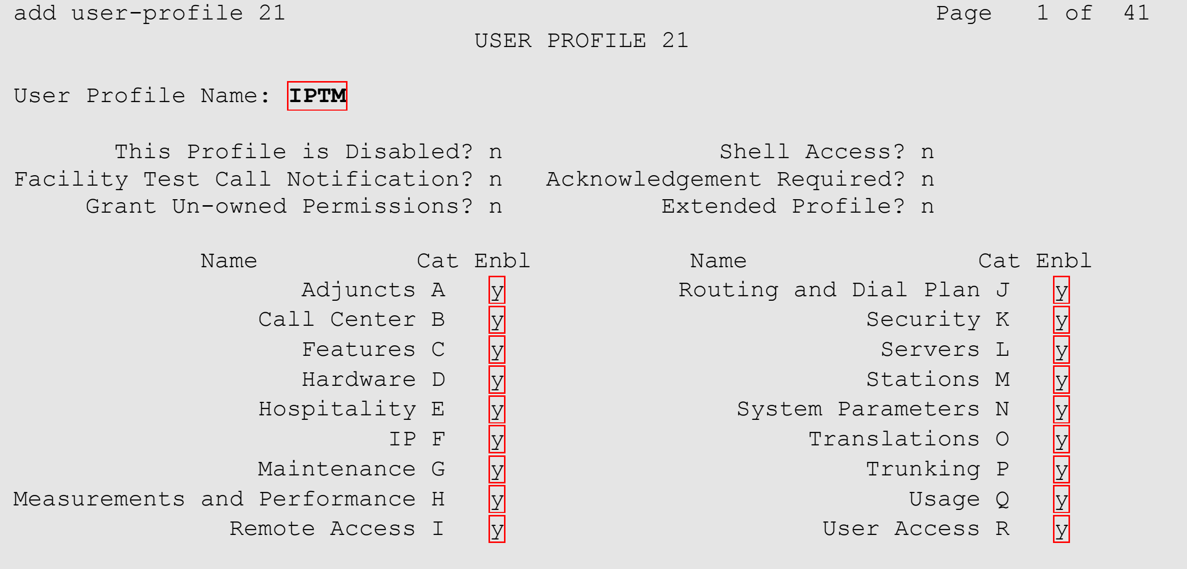
5. Configure Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with Integrated Research PROGNOSIS IP Telephony Manager. This includes creating a login account and a SAT User Profile for PROGNOSIS to access Communication Manager and enabling RTCP and CDR reporting. The steps are repeated for each Communication Manager system, ESS and LSP Servers.

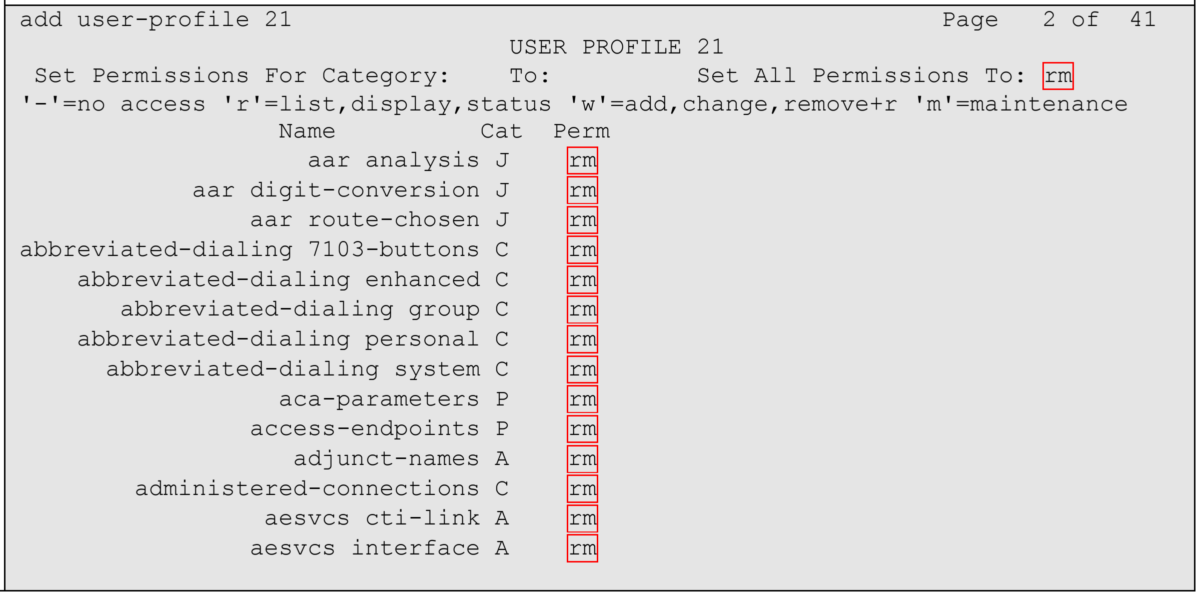
5.1. Configure SAT User Profile

A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As PROGNOSIS IP Telephony Manager does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the PROGNOSIS login account.

Step	Description
1.	Enter the **add user-profile *n*** command, where ***n*** is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**. In this configuration, the user profile 21 is created.



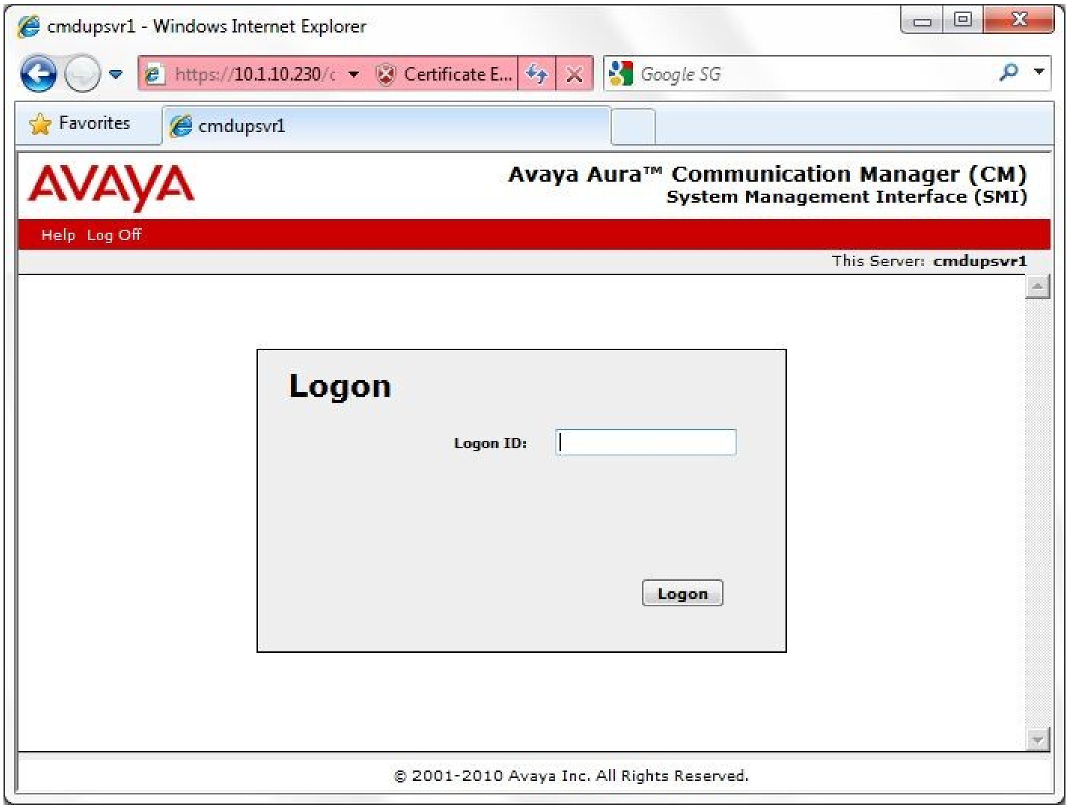
```
add user-profile 21                                             Page   1 of   41
                                USER PROFILE 21

User Profile Name: IPTM

       This Profile is Disabled? n               Shell Access? n
Facility Test Call Notification? n   Acknowledgement Required? n
     Grant Un-owned Permissions? n           Extended Profile? n

             Name           Cat Enbl          Name                Cat Enbl
                    Adjuncts A   y           Routing and Dial Plan J   y
                 Call Center B   y                        Security K   y
                    Features C   y                         Servers L   y
                    Hardware D   y                        Stations M   y
                 Hospitality E   y               System Parameters N   y
                          IP F   y                    Translations O   y
                 Maintenance G   y                        Trunking P   y
Measurements and Performance H   y                           Usage Q   y
               Remote Access I   y                     User Access R   y
```

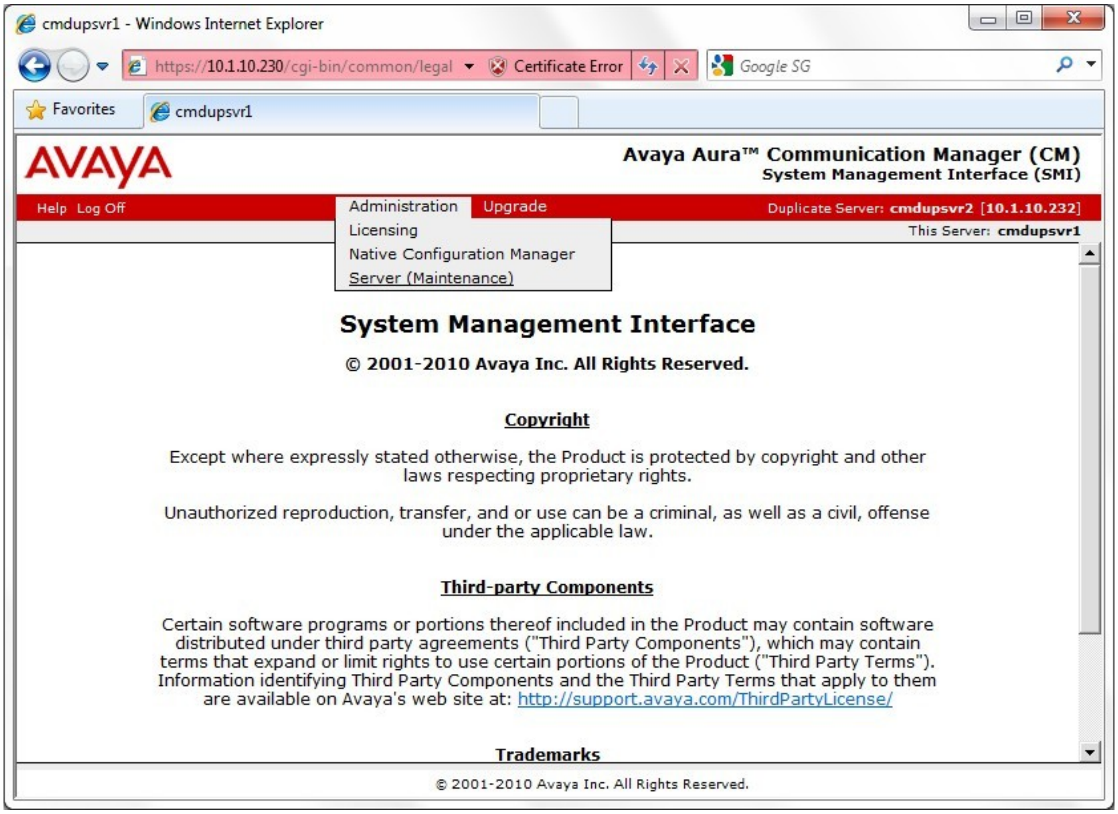
Step	Description
2.	On **Pages 2** to **41** of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile. 

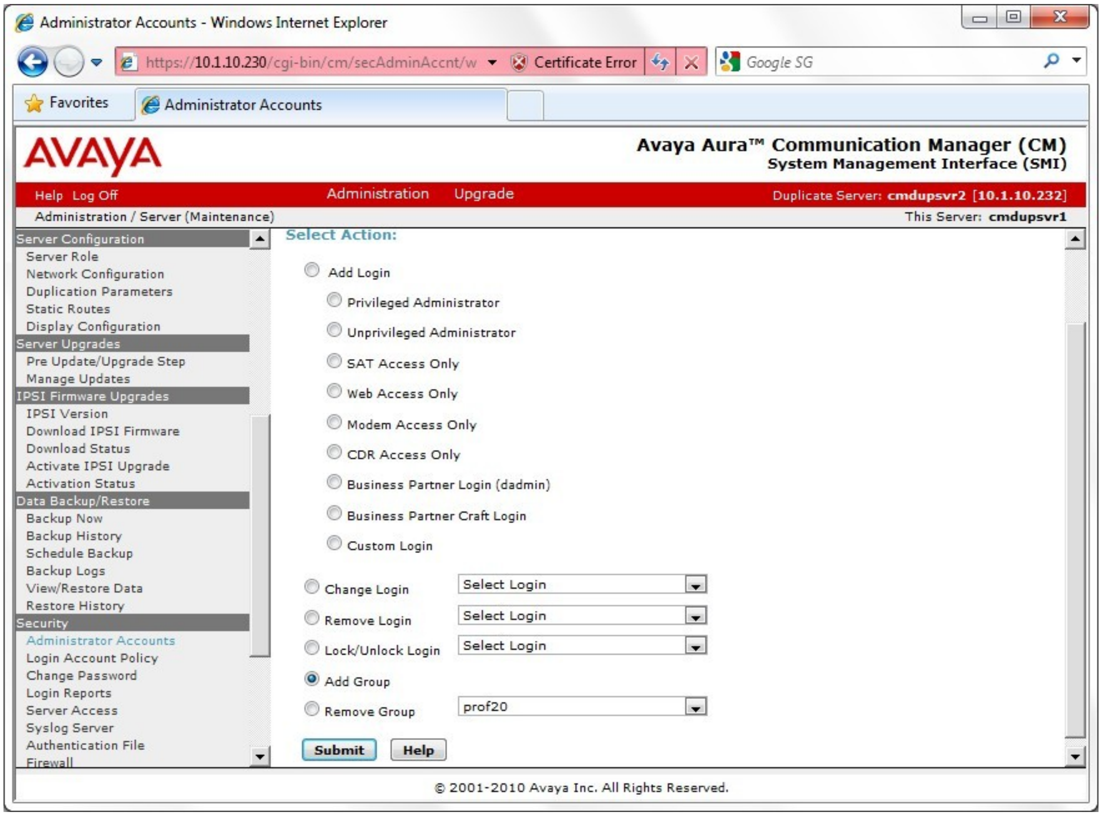
```
add user-profile 21                                             Page   2 of  41
                                  USER PROFILE 21
 Set Permissions For Category:    To:          Set All Permissions To: rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                    aar analysis J    rm
            aar digit-conversion J    rm
                aar route-chosen J    rm
abbreviated-dialing 7103-buttons C    rm
    abbreviated-dialing enhanced C    rm
       abbreviated-dialing group C    rm
    abbreviated-dialing personal C    rm
      abbreviated-dialing system C    rm
                  aca-parameters P    rm
                access-endpoints P    rm
                   adjunct-names A    rm
        administered-connections C    rm
                 aesvcs cti-link A    rm
                aesvcs interface A    rm
```

5.2. Configure Login Group

Create an Access-Profile Group to correspond to the SAT User Profile created in **Section 5.1**.

Step	Description
1.	Using a web browser, enter https://<IP address of Avaya Server> to connect to the Avaya Server being configured and log in using appropriate credentials.  cmdupsvr1 - Windows Internet Explorer https://10.1.10.230/c Certificate E... Google SG Favorites cmdupsvr1 AVAYA Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Help Log Off This Server: cmdupsvr1 Logon Logon ID: Logon © 2001-2010 Avaya Inc. All Rights Reserved.

Step	Description
2.	Click **Administration > Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.  cmdupsvr1 - Windows Internet Explorer https://10.1.10.230/cgi-bin/common/legal Certificate Error Google SG Favorites cmdupsvr1 AVAYA Help Log Off Administration Upgrade Licensing Native Configuration Manager Server (Maintenance) Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Duplicate Server: **cmdupsvr2 [10.1.10.232]** This Server: **cmdupsvr1** **System Management Interface** **© 2001-2010 Avaya Inc. All Rights Reserved.** **Copyright** Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law. **Third-party Components** Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/ **Trademarks** © 2001-2010 Avaya Inc. All Rights Reserved.

Step	Description
3.	From the navigation panel on the left side, click **Administrator Accounts** under **Security**. Select **Add Group** and click **Submit**. 

Select Action:

○ Add Login

- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ Modem Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login Select Login

○ Remove Login Select Login

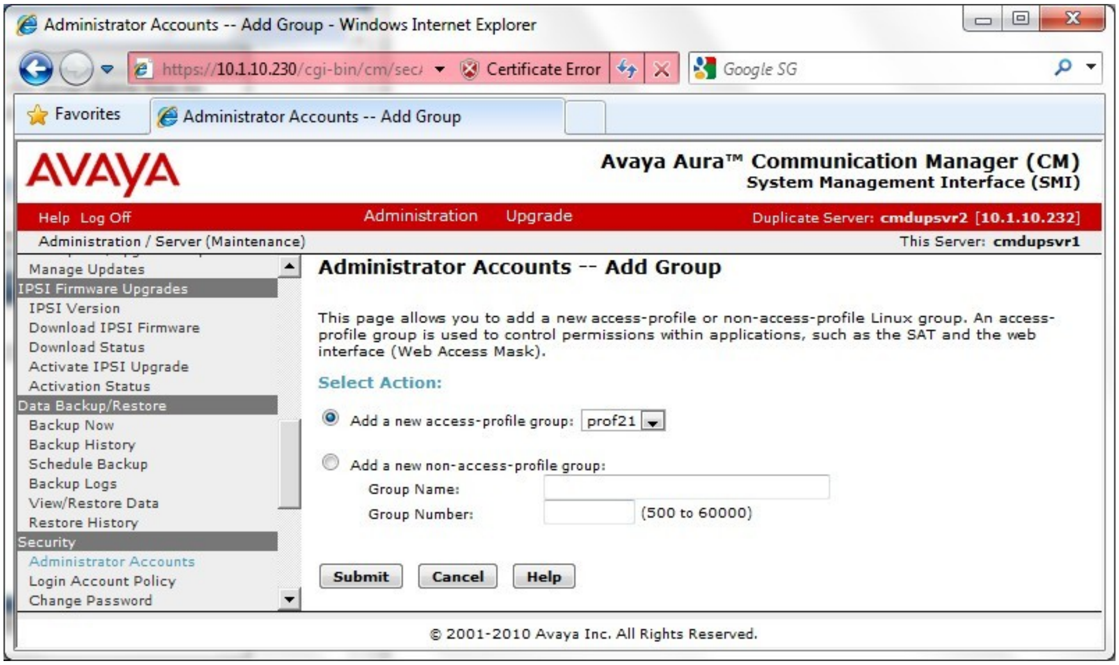
○ Lock/Unlock Login Select Login

● Add Group

○ Remove Group prof20

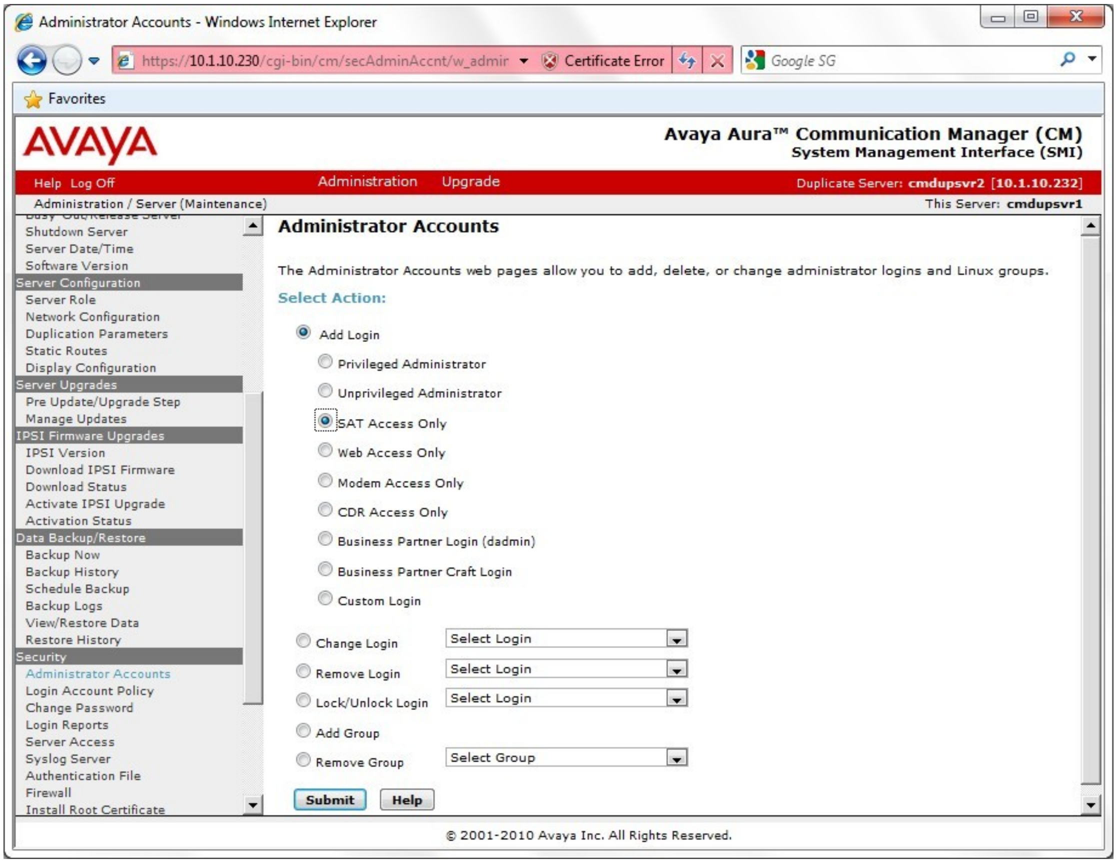
Submit Help

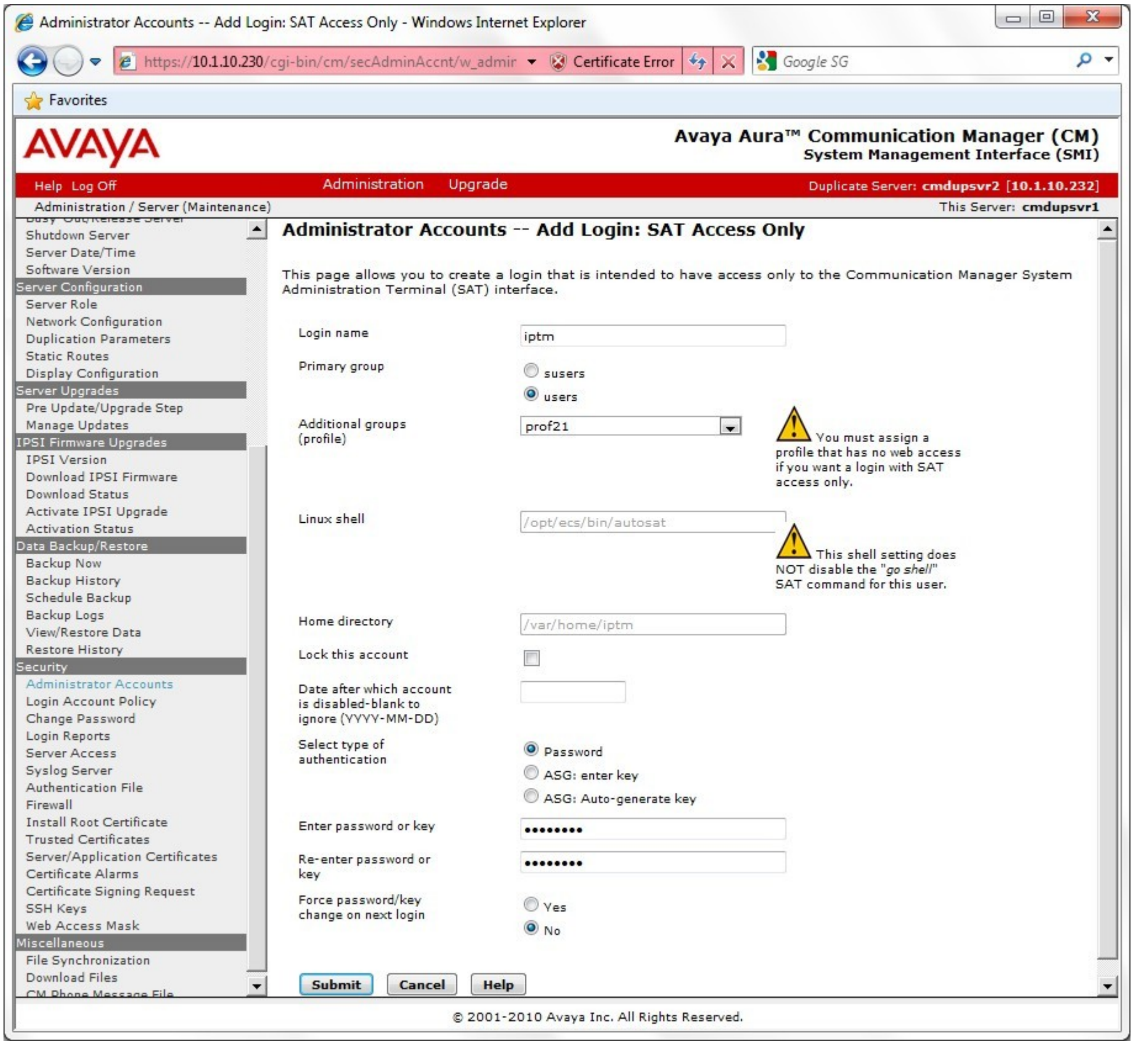
© 2001-2010 Avaya Inc. All Rights Reserved.

Step	Description
4.	Select **Add a new access-profile group** and select **prof21** from the drop-down box to correspond to the user-profile created in **Section 5.1 Step 1**. Click **Submit**. This completes the creation of the login group.  Administrator Accounts -- Add Group - Windows Internet Explorer https://10.1.10.230/cgi-bin/cm/sec/ Certificate Error Google SG Favorites Administrator Accounts -- Add Group AVAYA Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Upgrade Duplicate Server: cmdupsvr2 [10.1.10.232] Administration / Server (Maintenance) This Server: cmdupsvr1 Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password **Administrator Accounts -- Add Group** This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile group is used to control permissions within applications, such as the SAT and the web interface (Web Access Mask). Select Action: ● Add a new access-profile group: prof21 ○ Add a new non-access-profile group: Group Name: Group Number: (500 to 60000) Submit Cancel Help © 2001-2010 Avaya Inc. All Rights Reserved.

5.3. Configure Login

Create a login account for PROGNOSIS to access the Communication Manager SAT.

Step	Description
1.	From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.  Administrator Accounts - Windows Internet Explorer https://10.1.10.230/cgi-bin/cm/secAdminAccnt/w_admir Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Duplicate Server: cmdupsvr2 [10.1.10.232] Administration / Server (Maintenance) This Server: cmdupsvr1 **Administrator Accounts** The Administrator Accounts web pages allow you to add, delete, or change administrator logins and Linux groups. Select Action: ● Add Login ○ Privileged Administrator ○ Unprivileged Administrator ● SAT Access Only ○ Web Access Only ○ Modem Access Only ○ CDR Access Only ○ Business Partner Login (dadmin) ○ Business Partner Craft Login ○ Custom Login ○ Change Login — Select Login ○ Remove Login — Select Login ○ Lock/Unlock Login — Select Login ○ Add Group ○ Remove Group — Select Group Submit Help © 2001-2010 Avaya Inc. All Rights Reserved.

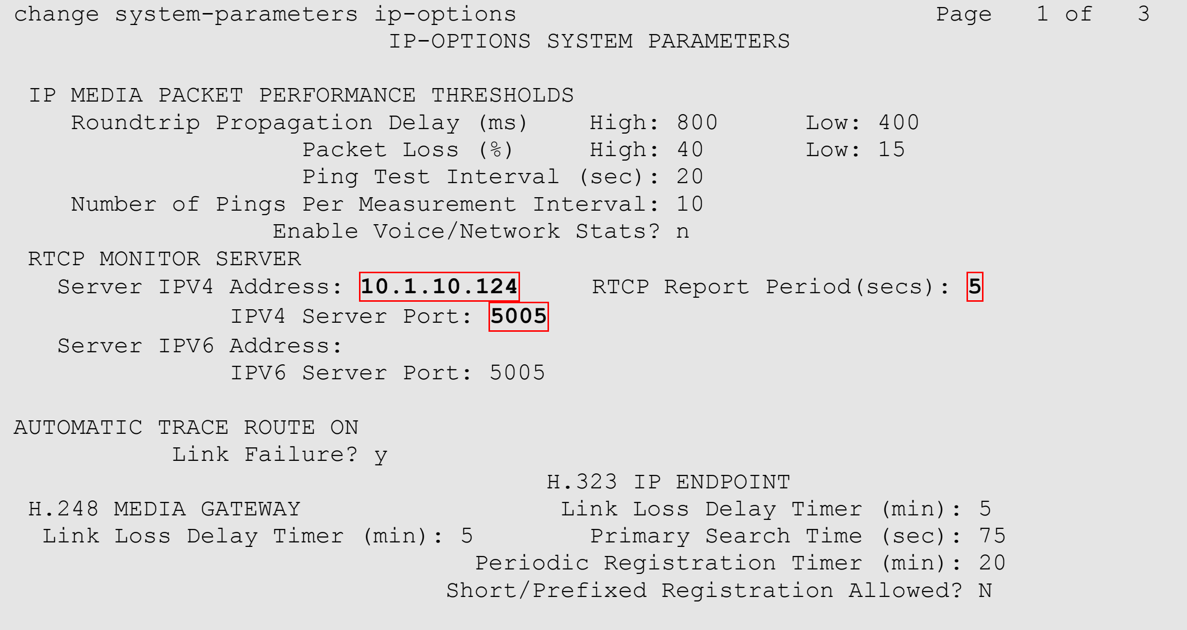
Step	Description
2.	For the field **Login name**, enter a login to be used by PROGNOSIS. In this configuration, the login **iptm** is created. Configure the other parameters for the login as follows: - **Primary group**: Select **users** [Limits the permissions of the login] - **Additional groups (profile)**: **prof21** [Select the login group created in **Section 5.2 Step 4**.] - **Select type of authentication:** Select **Password** [Uses a password for authentication.] - **Enter password or key / Re-enter password or key** [Define the password.] - **Force password/key change on next login**: Select **No** Click **Submit** to continue. This completes the configuration of the login.  Administrator Accounts -- Add Login: SAT Access Only - Windows Internet Explorer https://10.1.10.230/cgi-bin/cm/secAdminAccnt/w_admir Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Duplicate Server: **cmdupsvr2 [10.1.10.232]** Administration / Server (Maintenance) This Server: **cmdupsvr1** **Administrator Accounts -- Add Login: SAT Access Only** This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface. Login name: iptm Primary group: ○ susers ● users Additional groups (profile): prof21 You must assign a profile that has no web access if you want a login with SAT access only. Linux shell: /opt/ecs/bin/autosat This shell setting does NOT disable the "*go shell*" SAT command for this user. Home directory: /var/home/iptm Lock this account: □ Date after which account is disabled-blank to ignore (YYYY-MM-DD): Select type of authentication: ● Password ○ ASG: enter key ○ ASG: Auto-generate key Enter password or key: •••••••• Re-enter password or key: •••••••• Force password/key change on next login: ○ Yes ● No © 2001-2010 Avaya Inc. All Rights Reserved. Certificate Error Google SG Favorites AVAYA Help Log Off Administration Upgrade Shutdown Server Server Date/Time Software Version Server Configuration Server Role Network Configuration Duplication Parameters Static Routes Display Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password Login Reports Server Access Syslog Server Authentication File Firewall Install Root Certificate Trusted Certificates Server/Application Certificates Certificate Alarms Certificate Signing Request SSH Keys Web Access Mask Miscellaneous File Synchronization Download Files Submit Cancel Help

5.4. Configure RTCP Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the PROGNOSIS server. This is done through the SAT interface.

Step **Description**

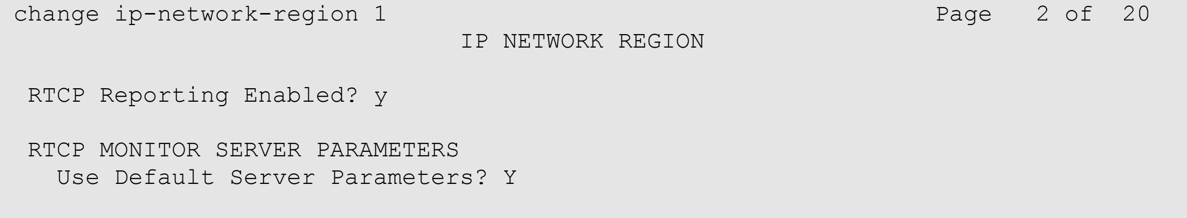
1. Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Server IPV4 Address** to the IP address of the PROGNOSIS IP Telephony Manager server. Set **IPV4 Server Port** to ***5005*** and **RTCP Report Period (secs)** to ***5***.



```
change system-parameters ip-options                             Page   1 of   3
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address: 10.1.10.124     RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                     H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                  Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5        Primary Search Time (sec): 75
                                Periodic Registration Timer (min): 20
                              Short/Prefixed Registration Allowed? N
```

2. Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. On **Page 2**, set **RTCP Reporting Enabled** to **y** and **Use Default Server Parameters** to ***y***.

   Note: Only one RTCP MONITOR SERVER can be configured per IP network region.



```
change ip-network-region 1                                      Page   2 of  20
                               IP NETWORK REGION

 RTCP Reporting Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? Y
```

3. Repeat **Step 2** for all IP network regions that are required to be monitored.

5.5. Configure CDR Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the CDR information, configure Communication Manager to send CDR information to the IP address of the PROGNOSIS server.

Step **Description**

1. Enter the **change ip-interface procr** command to enable the processor-ethernet interface on the Avaya Server. Set **Enable Interface** to **y**. This interface will be used by Communication Manager to send out the CDR information.

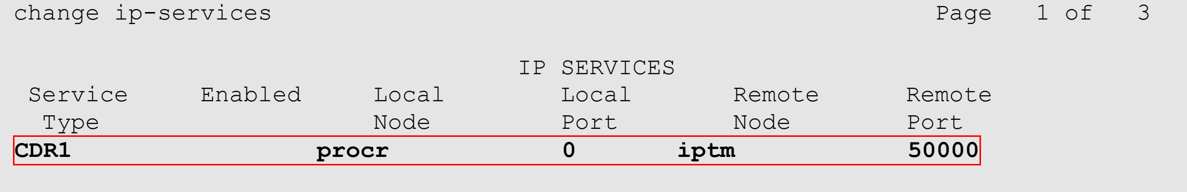
```
change ip-interface procr                                       Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                          Target socket load: 19660

      Enable Interface? y                                 Allow H.323 Endpoints? y
                                                           Allow H.248 Gateways? y
        Network Region: 1                                   Gatekeeper Priority: 5


                                 IPV4 PARAMETERS
             Node Name: procr                        IP Address: 10.1.10.230


           Subnet Mask: /24
```

2. Enter the **change node-names ip** command to add a new node name for the PROGNOSIS server. In this configuration, the name **iptm** is added with the IP address specified as **10.1.10.124**. Note also the node name **procr** which is automatically added.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
CLAN-01a02          10.1.50.21
CLAN-01a03          10.1.50.22
CLAN-02a02          10.1.10.21
DefaultRouter       10.1.50.1
MEDPRO-01a07        10.1.50.31
MEDPRO-01a08        10.1.50.32
MEDPRO-01a09        10.1.50.33
MEDPRO-02a13        10.1.10.31
MEDPRO-02a14        10.1.10.32
VAL-01a11           10.1.50.41
cm6ess              10.1.10.239
default             0.0.0.0
iptm                10.1.10.124
procr               10.1.10.230
procr6              ::
router10            10.1.10.1
```

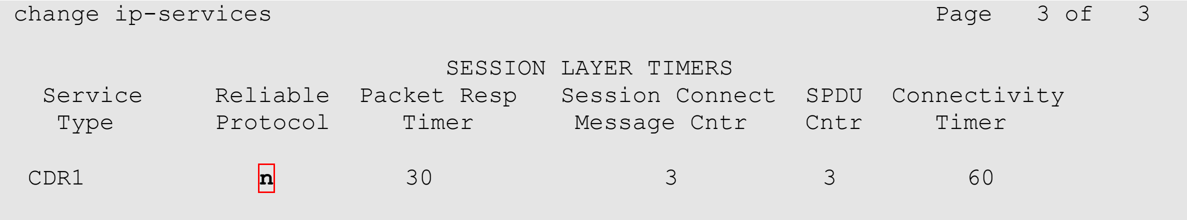
Step	Description
3.	Enter the **change ip-services** command to define the CDR link. To define a primary CDR link, the following information should be provided:

- **Service Type: CDR1** [Note: If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node: procr** [Note: Communication Manager will use the processor-ethernet interface to send out the CDR.]
- **Local Port: 0 [**Note: The Local Port is set to 0 because Communication Manager initiates the CDR link.]
- **Remote Node: iptm** [Note: The Remote Node is set to the node name previously defined in **Step 1**.]
- **Remote Port: 50000** [Note: The Remote Port may be set to a value between 5000 and 64500 inclusive. **50000** is the default port number used by PROGNOSIS and the PROGNOSIS server uses the same port number for all Avaya Servers sending CDR information to it.]



```
change ip-services                                                Page   1 of   3

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
CDR1                    procr           0       iptm              50000
```

On **Page 3** of the IP SERVICES form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.



```
change ip-services                                                Page   3 of   3

                              SESSION LAYER TIMERS
  Service      Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type        Protocol     Timer       Message Cntr    Cntr     Timer

 CDR1             n         30                 3          3          60
```

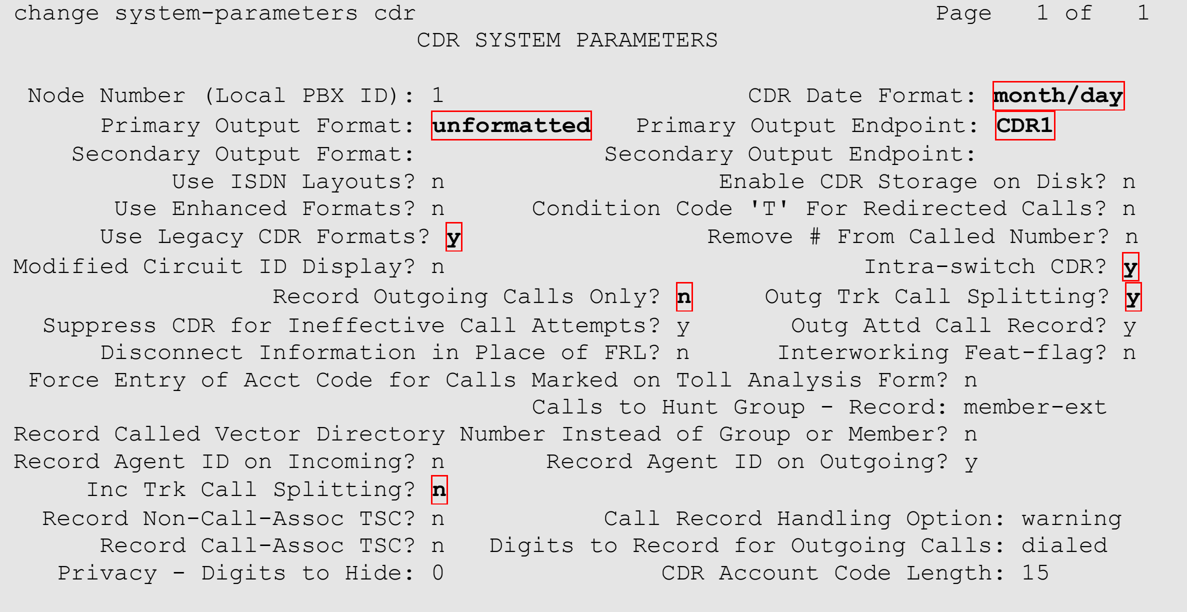
Step **Description**

4. Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.

- **CDR Date Format**: **month/day**
- **Primary Output Format**: **unformatted** [Note: This value is used to configure PROGNOSIS in **Section 5 Step 3**.]
- **Primary Output Endpoint**: **CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See **Reference [2]** for a full explanation of each field. The test configuration used some of the more common fields described below.

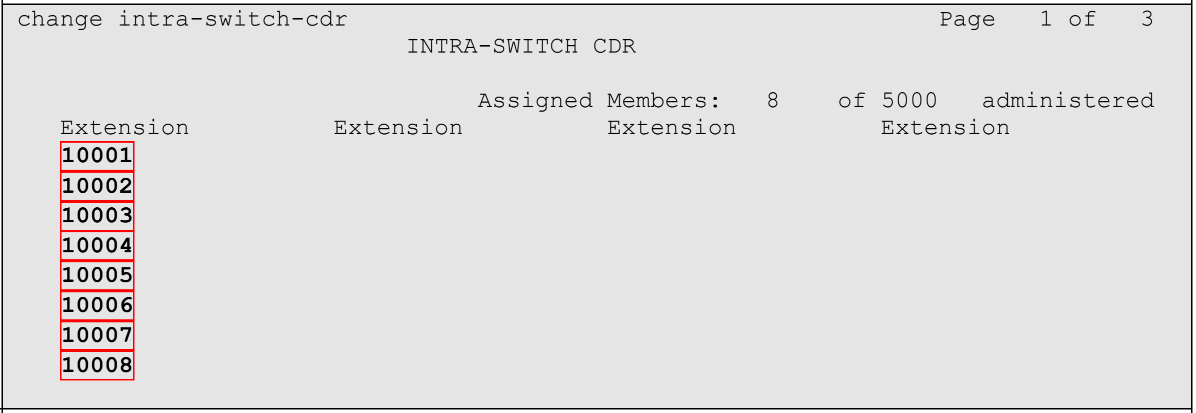
- **Use Legacy CDR Formats? y** [Note: Specify the use of the Communication Manager 3.x ("legacy") formats in the CDR records produced by the system.]
- **Intra-switch CDR: y** [Note: Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form.]
- **Record Outgoing Calls Only? n** [Note: Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting? y** [Note: Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting? n** [Note: Do not allow a separate call record for any portion of an incoming call that is transferred or conferenced.]



```
change system-parameters cdr                                    Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                     CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format:             Secondary Output Endpoint:
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? y                 Remove # From Called Number? n
Modified Circuit ID Display? n                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
```

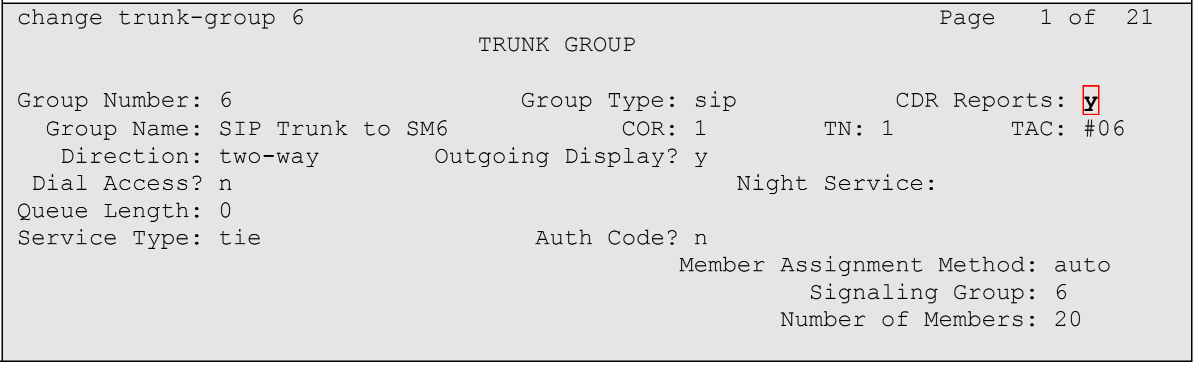
Step **Description**

5. If the **Intra-switch CDR** field is set to **y** on **Page 1** of the CDR SYSTEM PARAMETERS form, then enter the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail recording. In the **Assigned Members** field, enter the specific extensions whose usage will be tracked with the CDR records.



```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   8    of 5000   administered
   Extension            Extension           Extension           Extension
   10001
   10002
   10003
   10004
   10005
   10006
   10007
   10008
```

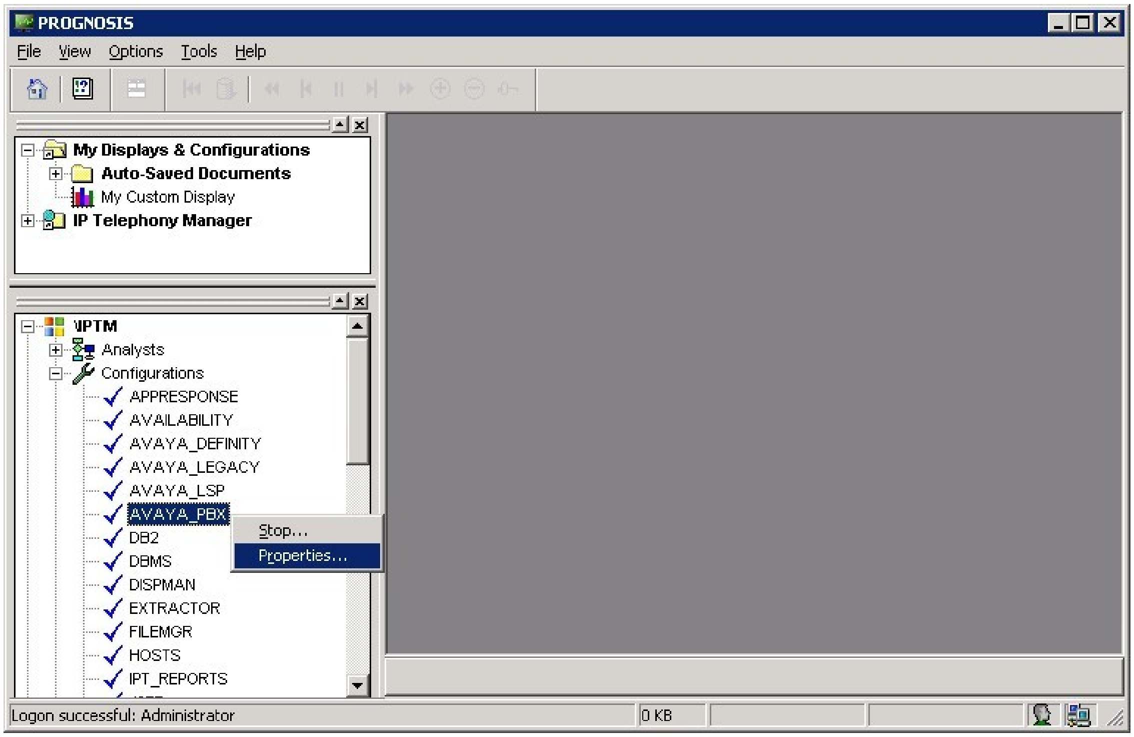
6. For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the **change trunk-group n** command, where **n** is the trunk group number, to verify that the **CDR Reports** field is set to **y**. Repeat for all trunk groups to be reported.



```
change trunk-group 6                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SM6            COR: 1        TN: 1        TAC: #06
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 6
                                                     Number of Members: 20
```

6. Configure Integrated Research PROGNOSIS IP Telephony Manager

This section describes the configuration of PROGNOSIS IP Telephony Manager required to interoperate with Communication Manager.

Step	Description
1.	On PROGNOSIS IP Telephony Manager server, click **Start > All Programs > PROGNOSIS IP Telephony Manager > IP Telephony Manager GUI** to start the IP Telephony Manager GUI application. Enter a valid Windows user account and password to log in.
2.	To configure the Communication Manager systems to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA_PBX** and select **Properties**.  PROGNOSIS File View Options Tools Help My Displays & Configurations Auto-Saved Documents My Custom Display IP Telephony Manager \IPTM Analysts Configurations APPRESPONSE AVAILABILITY AVAYA_DEFINITY AVAYA_LEGACY AVAYA_LSP AVAYA_PBX DB2 DBMS DISPMAN EXTRACTOR FILEMGR HOSTS IPT_REPORTS Stop... Properties... 0 KB Logon successful: Administrator

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

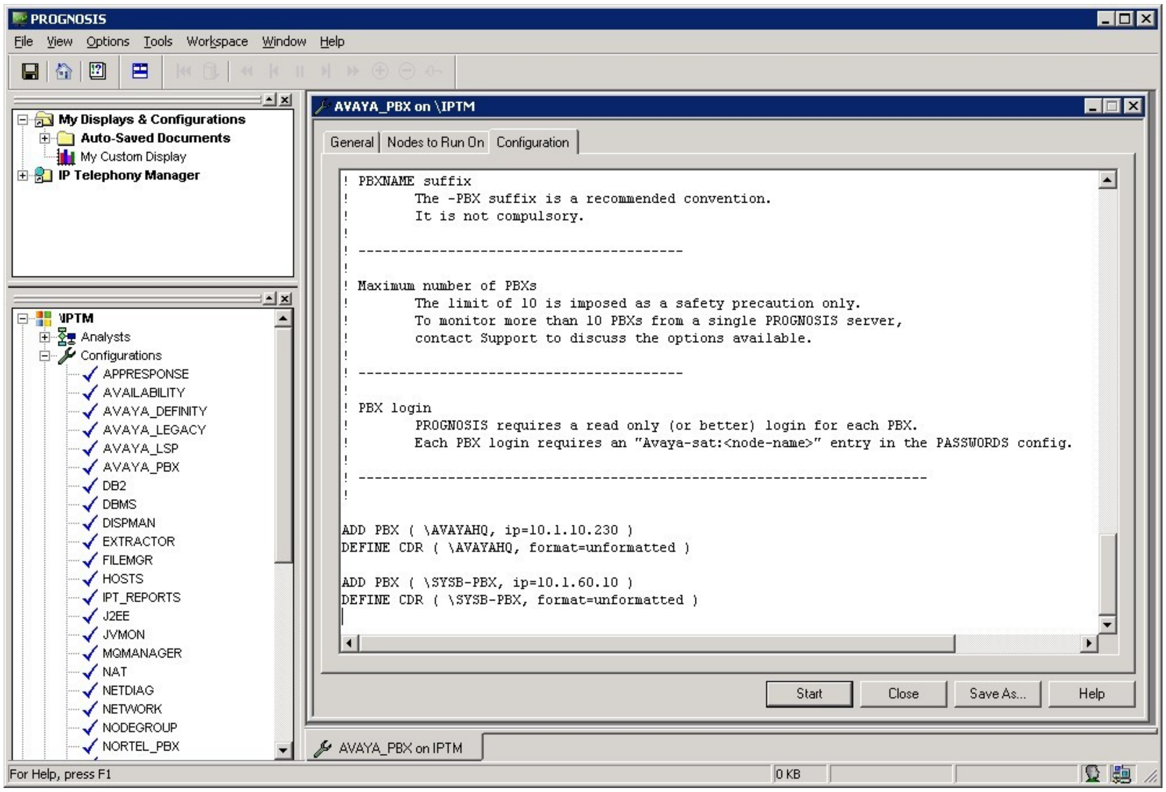
In the **Configuration** tab, add an entry for each Communication Manager system to be managed. The template to add a system is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the two Communication Manager systems with the names **AVAYAHQ** and **SYSB-PBX** and with the IP addresses of the Avaya Servers **10.1.10.230** and **10.1.60.10** respectively. The PROGNOSIS Monitoring Node will use SSH to connect to port 5022 of the Avaya Servers.

```
ADD PBX ( \AVAYAHQ, ip=10.1.10.230 )
ADD PBX ( \SYSB-PBX, ip=10.1.60.10 )
```

Define the CDR format to match the settings configured on Communication Manager in **Section 5.5 Step 2 and 3** respectively.

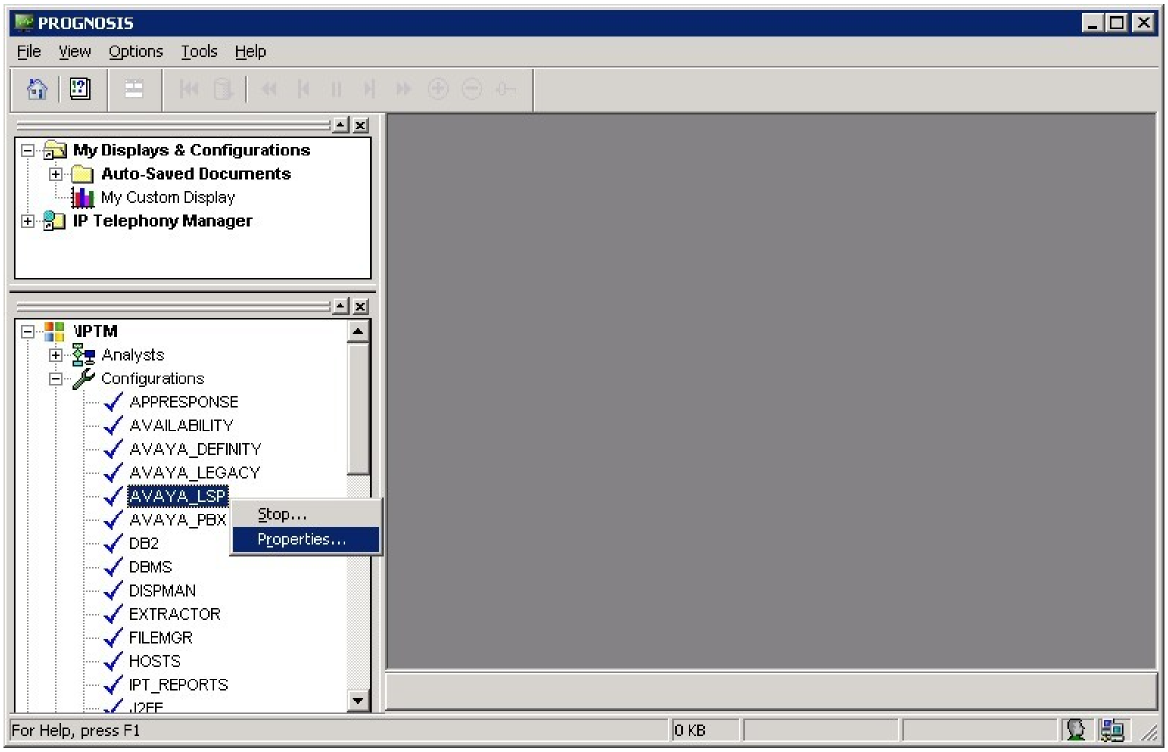
```
DEFINE CDR ( \AVAYAHQ, format=unformatted )
DEFINE CDR ( \SYSB-PBX, format=unformatted )
```

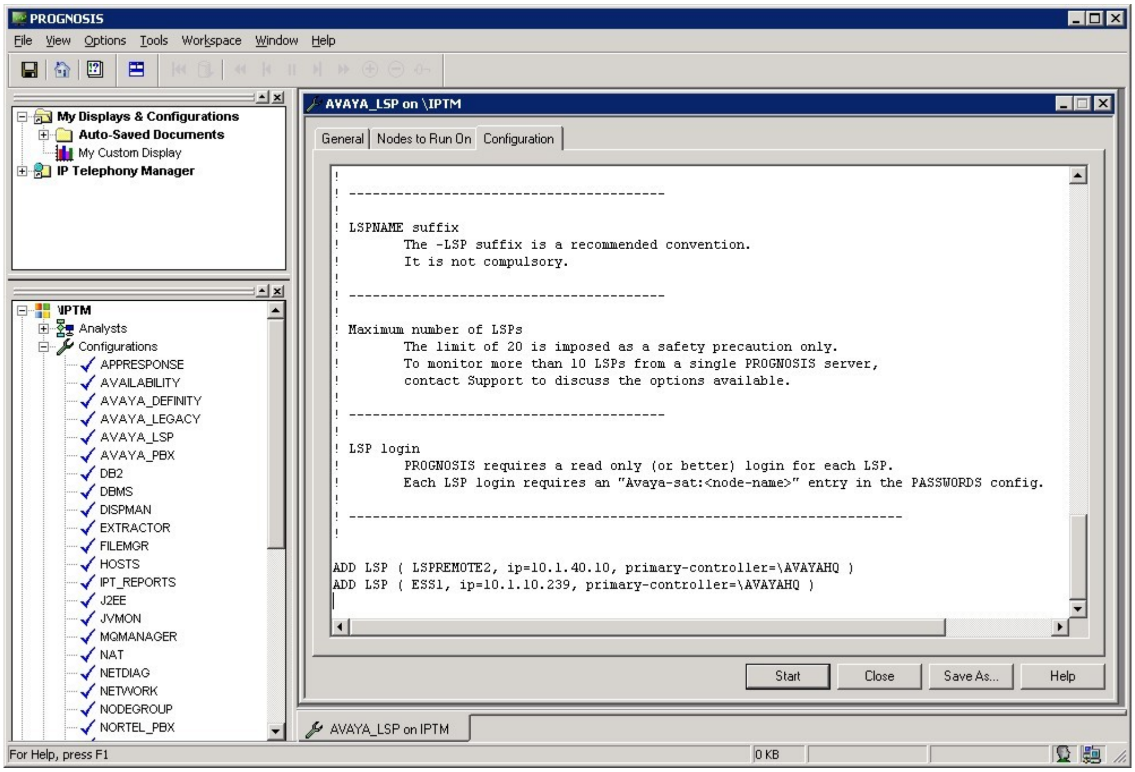
Click **Start** to proceed.



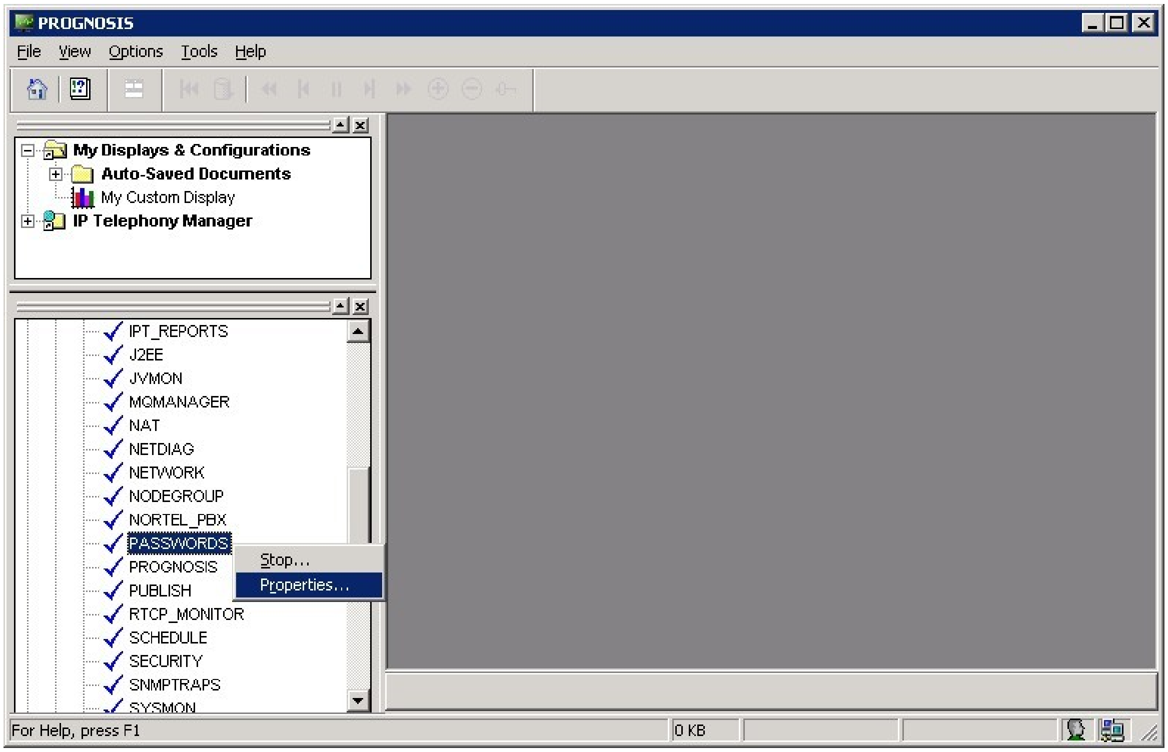
```
! PBXNAME suffix
!        The -PBX suffix is a recommended convention.
!        It is not compulsory.
!
! ----------------------------------------
!
! Maximum number of PBXs
!        The limit of 10 is imposed as a safety precaution only.
!        To monitor more than 10 PBXs from a single PROGNOSIS server,
!        contact Support to discuss the options available.
!
! ----------------------------------------
!
! PBX login
!        PROGNOSIS requires a read only (or better) login for each PBX.
!        Each PBX login requires an "Avaya-sat:<node-name>" entry in the PASSWORDS config.
!
! ----------------------------------------------------------------------
!

ADD PBX ( \AVAYAHQ, ip=10.1.10.230 )
DEFINE CDR ( \AVAYAHQ, format=unformatted )

ADD PBX ( \SYSB-PBX, ip=10.1.60.10 )
DEFINE CDR ( \SYSB-PBX, format=unformatted )
```

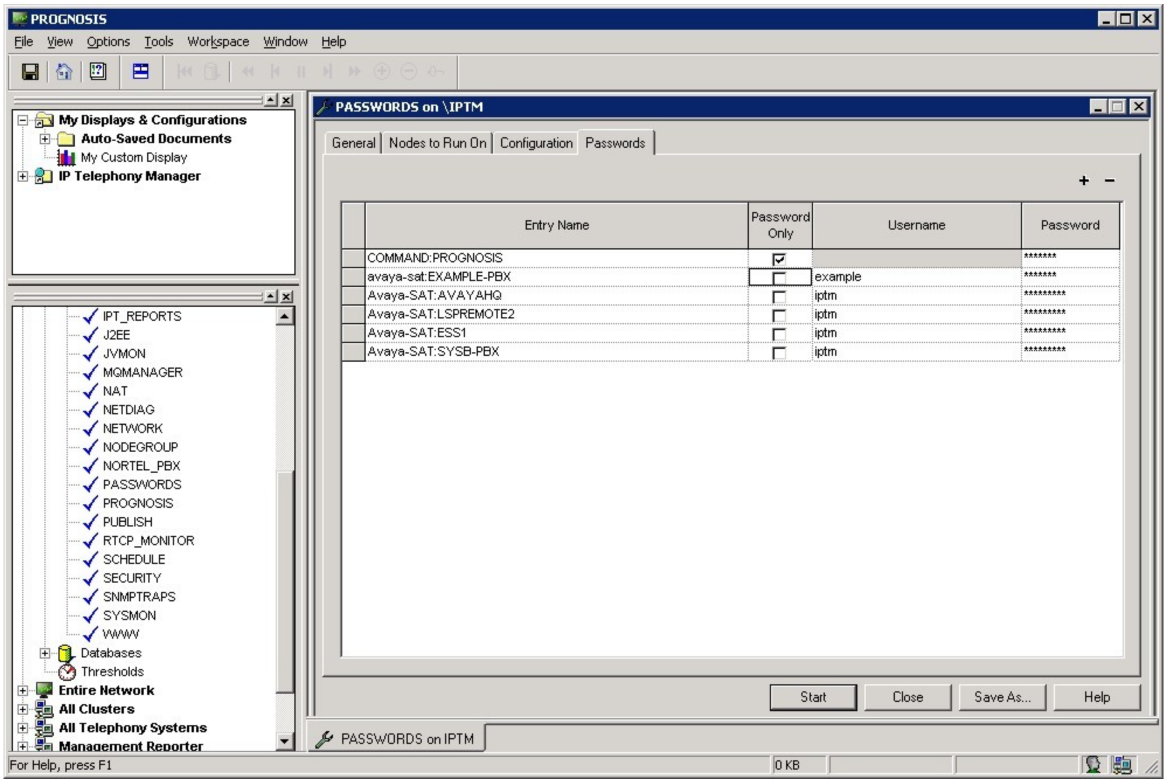
</td></tr>
</table>

Step	Description
4.	To configure the ESS and LSP Servers to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA_LSP** and select **Properties**. 

Step	Description
5.	In the **Configuration** tab, add an entry for each ESS or LSP Servers to be monitored. The template to add the server is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the ESS and LSP Servers with the names **LSPREMOTE2** and **ESS1** and with the IP addresses of **10.1.40.10** and **10.1.10.239** respectively, both belonging to the **AVAYAHQ** Communication Manager system. ADD LSP (LSPREMOTE2, ip=10.1.40.10, primary-controller=\AVAYAHQ) ADD LSP (ESS1, ip=10.1.10.239, primary-controller=\AVAYAHQ) Click **Start** to proceed. 

```
!
! ----------------------------------------
!
! LSPNAME suffix
!        The -LSP suffix is a recommended convention.
!        It is not compulsory.
!
! ----------------------------------------
!
! Maximum number of LSPs
!        The limit of 20 is imposed as a safety precaution only.
!        To monitor more than 10 LSPs from a single PROGNOSIS server,
!        contact Support to discuss the options available.
!
! ----------------------------------------
!
! LSP login
!        PROGNOSIS requires a read only (or better) login for each LSP.
!        Each LSP login requires an "Avaya-sat:<node-name>" entry in the PASSWORDS config.
!
! ------------------------------------------------------------------
!

ADD LSP ( LSPREMOTE2, ip=10.1.40.10, primary-controller=\AVAYAHQ )
ADD LSP ( ESS1, ip=10.1.10.239, primary-controller=\AVAYAHQ )
```

Step	Description
6.	To configure the SAT login account and password, expand **Configurations** of the Monitoring Node, right-click on **PASSWORDS** and select **Properties**.  PROGNOSIS File View Options Tools Help My Displays & Configurations Auto-Saved Documents My Custom Display IP Telephony Manager IPT_REPORTS J2EE JVMON MQMANAGER NAT NETDIAG NETWORK NODEGROUP NORTEL_PBX PASSWORDS PROGNOSIS PUBLISH RTCP_MONITOR SCHEDULE SECURITY SNMPTRAPS SYSMON Stop... Properties... For Help, press F1 0 KB

Step	Description
7.	Click the + **'plus'** button to add a new password entry for each of the configured systems in **Steps 3** and **5**. The **Entry Name** must be of the form Avaya-SAT:<pbx-name>. For the system with the name **AVAYAHQ**, enter **Avaya-SAT:AVAYAHQ** for **Entry Name**, uncheck **Password Only**, and enter the login account created in **Section 5.3** for **Username** and **Password**. Repeat to add another three entries for the ESS and LSP Servers, and the second system **SYSB-PBX**. Click **Start** to proceed. 

Entry Name	Password Only	Username	Password
COMMAND:PROGNOSIS	☑		*******
avaya-sat:EXAMPLE-PBX	☐	example	*******
Avaya-SAT:AVAYAHQ	☐	iptm	*********
Avaya-SAT:LSPREMOTE2	☐	iptm	*********
Avaya-SAT:ESS1	☐	iptm	*********
Avaya-SAT:SYSB-PBX	☐	iptm	*********

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Integrated Research PROGNOSIS IP Telephony Manager.

7.1. Verify Communication Manager

Verify that PROGNOSIS IP Telephony Manager has established three concurrent SSH connections to the SAT by using the **status logins** command.

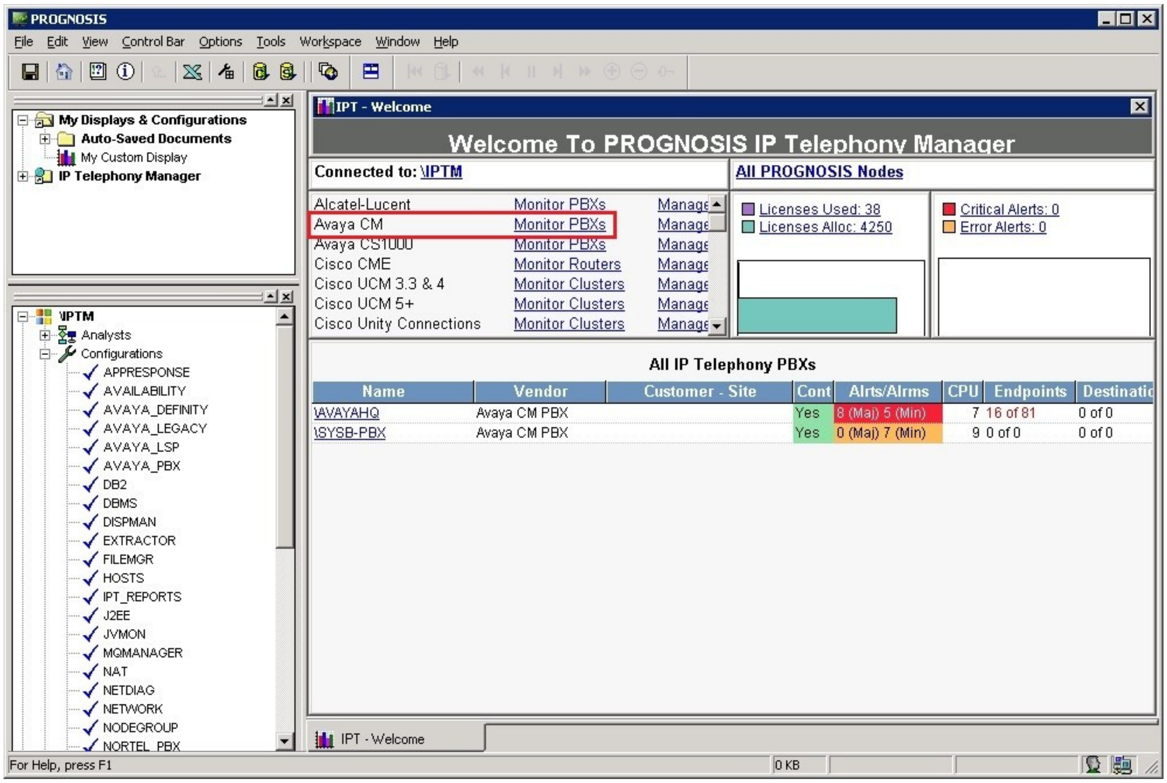
```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login     Profile   User's Address      Active Command              Session

 iptm        21                       list measurements summary        1
                     10.1.10.124
 iptm        21                       list registered-ip-stations      3
                     10.1.10.124
 iptm        21                       stat trunk 10                    4
                     10.1.10.124
*dadmin      2                        stat logins                      5
                     10.1.10.99
```

Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

```
status cdr-link
                              CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2011/04/14 17:16:20            0000/00/00 00:00:00
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK
```

7.2. Verify Integrated Research PROGNOSIS IP Telephony Manager

The following steps are done using the PROGNOSIS GUI.

Step	Description
1.	After logging into PROGNOSIS GUI, click on the **Home** button on the toolbar to display the **Welcome** screen. In the **Monitor** section, click **Avaya CM > Monitor PBXs** to display the list of Communication Manager Servers configured in **Section 6**. 

IPT - Welcome

Welcome To PROGNOSIS IP Telephony Manager

Connected to: \IPTM

All PROGNOSIS Nodes

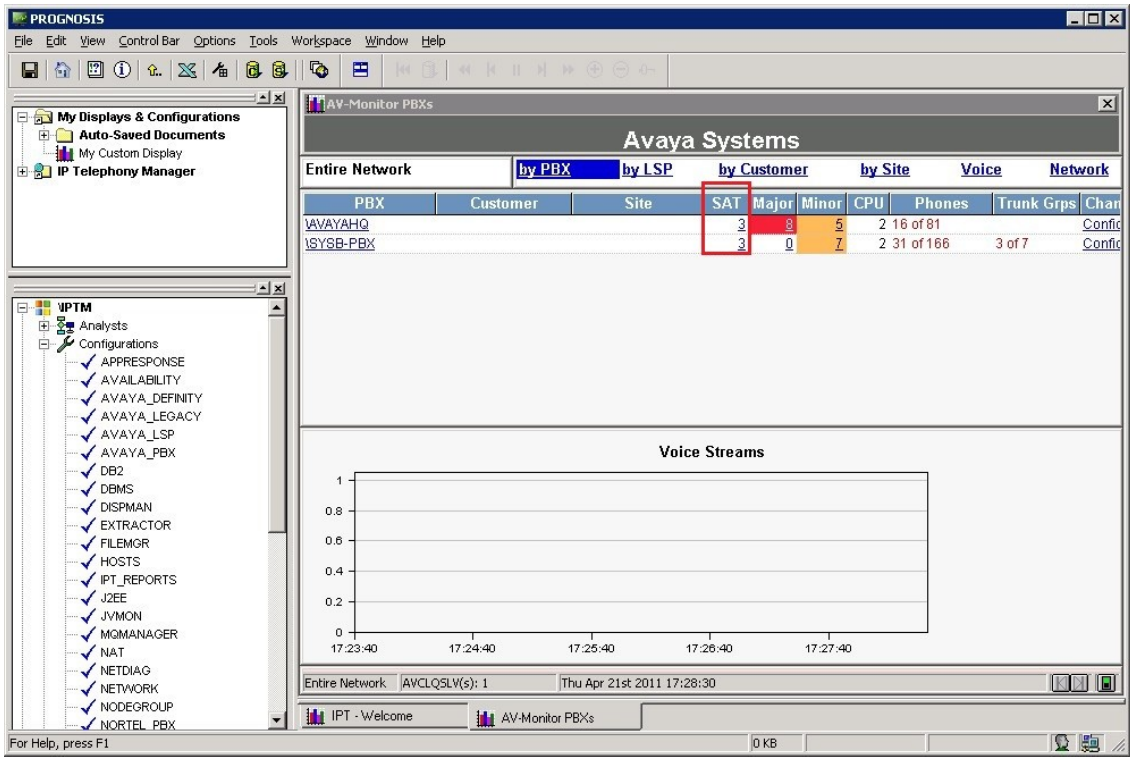
Alcatel-Lucent	Monitor PBXs	Manage
Avaya CM	Monitor PBXs	Manage
Avaya CS1000	Monitor PBXs	Manage
Cisco CME	Monitor Routers	Manage
Cisco UCM 3.3 & 4	Monitor Clusters	Manage
Cisco UCM 5+	Monitor Clusters	Manage
Cisco Unity Connections	Monitor Clusters	Manage

🟪 Licenses Used: 38
🟩 Licenses Alloc: 4250

🟥 Critical Alerts: 0
🟧 Error Alerts: 0

All IP Telephony PBXs

Name	Vendor	Customer - Site	Cont	Alrts/Alrms	CPU	Endpoints	Destinatio
\AVAYAHQ	Avaya CM PBX		Yes	8 (Maj) 5 (Min)	7	16 of 81	0 of 0
\SYSB-PBX	Avaya CM PBX		Yes	0 (Maj) 7 (Min)	9	0 of 0	0 of 0

Step	Description
2.	In the **Avaya Systems** page, verify that the **SAT** field for each configured Communication Manager shows **3** connections. 

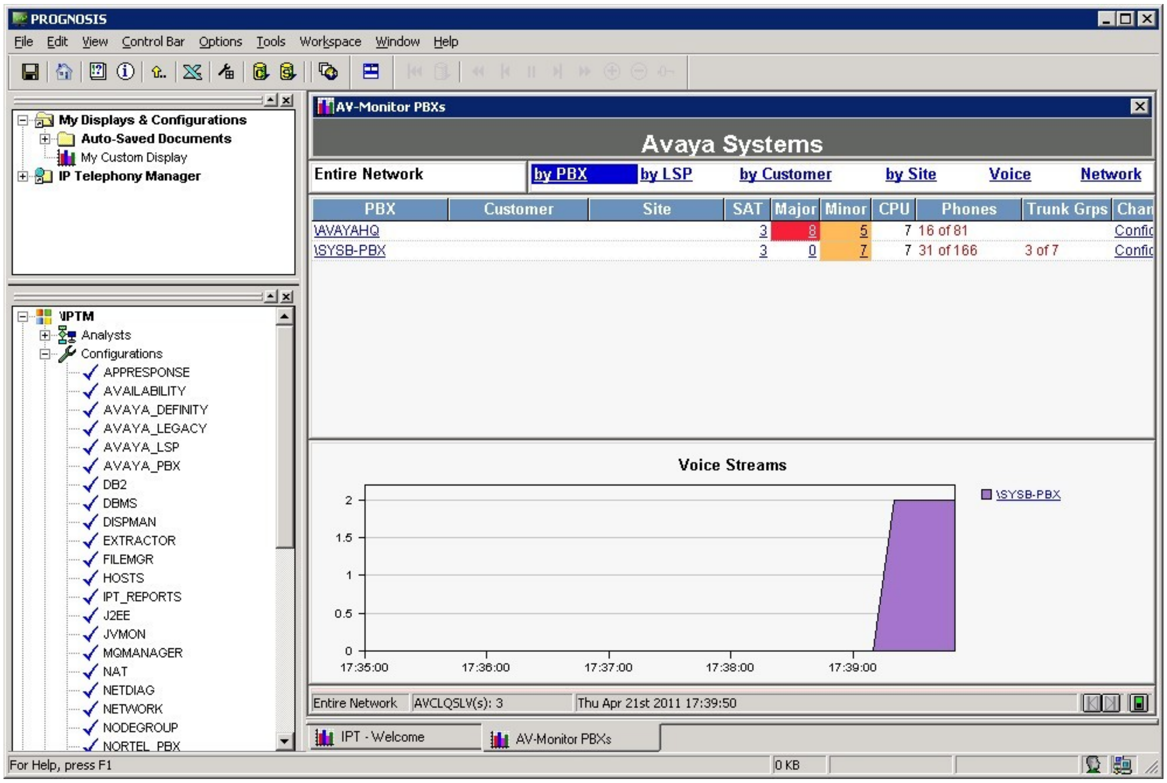
Avaya Systems

Entire Network | by PBX | by LSP | by Customer | by Site | Voice | Network

PBX	Customer	Site	SAT	Major	Minor	CPU	Phones	Trunk Grps	Chan
\AVAYAHQ			3	8	5	2	16 of 81		Confic
\SYSB-PBX			3	0	7	2	31 of 166	3 of 7	Confic

Entire Network | AVCLQSLV(s): 1 | Thu Apr 21st 2011 17:28:30

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>Make a call between two Avaya IP telephones that belong to an IP Network Region that has been configured to send RTCP information to the PROGNOSIS server. Verify that the <b>Voice Streams</b> section shows two active voice streams reflecting the quality of the call.



<table>
<tr><th>PBX</th><th>Customer</th><th>Site</th><th>SAT</th><th>Major</th><th>Minor</th><th>CPU</th><th>Phones</th><th>Trunk Grps</th><th>Chan</th></tr>
<tr><td>\AVAYAHQ</td><td></td><td></td><td>3</td><td>8</td><td>5</td><td>7</td><td>16 of 81</td><td></td><td>Confic</td></tr>
<tr><td>\SYSB-PBX</td><td></td><td></td><td>3</td><td>0</td><td>7</td><td>7</td><td>31 of 166</td><td>3 of 7</td><td>Confic</td></tr>
</table>

Entire Network | AVCLQSLV(s): 3 | Thu Apr 21st 2011 17:39:50

For Help, press F1 | 0 KB</td></tr>
</table>

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research PROGNOSIS IP Telephony Manager to interoperate with Avaya Aura® Communication Manager. In the configuration described in these Application Notes, PROGNOSIS IP Telephony Manager established SSH connections to the SAT to view the configurations of Communication Manager and to monitor for failures. PROGNOSIS IP Telephony Manager also processed the RTCP information to monitor the quality of IP calls and collected CDR information from the Communication Manager. During compliance testing, all test cases were completed successfully.

9. Additional References

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 6.0, Issue 8.0, June 2010, Document Number 555-245-205.
[2] *Administering Avaya Aura^{TM} Communication Manager*, June 2010, Release 6.0, Issue 6.0, Document Number 03-300509.

The following PROGNOSIS documents are provided by Integrated Research.

[3] *PROGNOSIS IP Telephony Manager 9.6 Installation and Configuration Guide*, September 2010.
[4] *PROGNOSIS IP Telephony Manager 9.6 User Guide Online Help*.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.